Amendments to the Drawings:

The attached replacement sheet of drawings includes changes to Fig. 1 and replaces the original sheet including Fig. 1.

In Figure 1, reference number 21 and a box were added to each of the boxes 20a-20c depicting data centers.

Attachments following last page of this Amendment:

Replacement Sheet (1 pages)
Annotated Sheet Showing Change(s) (0 pages)

REMARKS

The examiner objected to the drawings under 37 CFR 1.83(a) because they fail to show "software program 21" on page 5 lines 7-8 of Fig. 1, as described in the specification. Applicant had enclosed a proposed correction and now encloses herewith a replacement sheet showing software program 21 as well as a box added to the boxes 20a-20c depicting data centers. No new matter has been added.

Applicant has made clarifying amendments to the claims.

The examiner provisionally rejected Claims 1, 3-9, 11-19, 21-22, 24-27 under the judicially created doctrine of obviousness-type double patenting, as being unpatentable over claims 1-36 of co-pending Application No. 09/931,561.

Applicant traverses this rejection, since claim 1 of the instant case is claiming a sub-combination of the method and system claimed in the co-pending application. The control center in the instant claims is the central controller element of the method claim 1 in the co-pending application. Accordingly, the differences between the claims are that they are directed to different inventions. As such issuance of a patent on the subject matter of the instant case would not extend the monopoly of the claims in the co-pending case, and vice versa. Therefore, the rejection is improper and should be removed.

In response to Applicant's argument, the examiner stated that:

> **3. The rejection to claims 1,3-9, 11-19, 21-22, and 24-27 under the judicially created doctrine of obviousness-type double patenting, as being unpatentable over claims 1-36 of copending application No. 09/931,561 is appropriate because the difference in the scope, wherein the "control center" in the instant claims and "central controller element" of the method claim 1 in the co-pending application, is minor and patentably indistinct and are directed to the same inventive concept. The subject matter of the narrower claim is fully disclosed in and covered by the broader claim of the reference.**

Applicant disagrees with this analysis. Claim 1 of the present application recites: 1. "A control center system." The features of instant claim 1 are "a computer system … comprising, a communication device… the computer system executing: a process to analyze the statistical data … a process to identify gateways … and a filtering process … .

In contrast, claim 1 (and every independent claim of co-pending application '561 is directed to the overall system including the monitors, control center and the gateways recited either as positive elements in apparatus/article claims or as positive steps carried out on those elements in method claims.

The examiner having failed to show that the sub-combination would be obvious in view of the combination, it is submitted that the rejection is improper and should be removed.

Claim Rejections - 35 USC §102

The examiner rejected Claims 1, 9, 18, and 21 under 35 U.S.C. 102(e), as being anticipated by Greenwald et al. US PUB 2003/0149919 Al.

Applicant's claim 1, as previously presented, was distinct over Greenwald. Nevertheless, Applicant has amended the claims to clarify the subject matter claimed.

As amended, claim 1 is distinct over Greenwald since Greenwald neither describes nor suggests … a control center comprising a communication device, coupled to a physically separate network from the network that the data center is coupled to, to receive statistical data collected from network traffic flows collected by a plurality of monitors … the monitors sending the statistical data … over the physically separate network … the computer system executing … a process to analyze the statistical data … a process to identify gateways on the monitoring network that are sources of malicious traffic destined for the data center and a filtering process to eliminate the malicious traffic from entering the victim data center.

The examiner contends that Greenwald teaches … "a communication device (par. 0072; receiver fault diagnosis engine) to receive data from a plurality of monitors (plurality of fault engines on fig. 3 element 150) dispersed through the network … ." Applicant disagrees. The fault engines, as described by Greenwald, are not the recited monitors and thus Greenwald does not teach a communication device that receives data from a plurality of monitors, as claimed.

Rather, Greenwald teaches that "Fault diagnosis engine 101 provides a generic mechanism for fault handlers 150 to register for changes in the processing state of faults of a given fault type. Fault diagnosis engine 101 may employ any mechanism to specify registrations." Greenwald also describes the fault handlers 150 as: "Fault handlers 150 are registered for a particular fault type and state and, as part of the registration process, each fault

handler 150 has an integer priority value." Therefore, the so called fault handlers and the fault diagnosis engine are not collecting statistical information on network traffic nor analyzing that information in the control center. While, Greenwald also mentions that: "Fault handlers 150 may exist internal to the system, or reside externally in a separate process.", it is clear that Greenwald is not describing "to receive statistical data collected from network traffic flows collected by a plurality of monitors" and hence Greenwald is not describing the claimed "a communication device, coupled to a second separate network, that is physically separate from the network that the data center is coupled.

The examiner also contends that Greenwald teaches: "with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from (par. 0032, 0025 and fig. 6; in a physically different network) … ."Applicant also disagrees.

While the examiner relies on Fig. 6 and paragraphs 0025 and 0032 to supply this teaching, it is apparent that [0032] has no specific, relevant teaching directed to this feature and Fig. 6 merely shows a grouping of subnets in a network. Whether or not these subnets are viewed as different networks or not, it is clear that to the extent those subnets include "monitors," those monitors send data collected from the network over those subnets and hence Greenwald is not describing the claimed "a communication device, coupled to a physically separate network from the network that the data center is coupled to … .

The examiner also contends that Greenwald teaches:

> a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic (par. 0032 and 0035; determination of faults/DOS by fault engines and fault diagnosis engine), and ***analyzes and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center (par. 0032, 0104 and fig. 6B-C; packet filtering, monitor gateway preventing traffic from being*** transmitted from first to second device upon detection)." (emphasis in original).

Applicant also disagrees. While the examiner relies on Fig. 6b-c and paragraphs 0032 and 0104 to supply this teaching, it is apparent that [0032] has no specific, relevant teaching directed to this feature, and Figs. 6b-c merely show fault isolation and detection using a ping test. Whether or not these actions can be used to detect attacks, those techniques do not describe "a

process to analyze the statistical data from the plurality of monitors … a process to identify gateways on the monitoring network that are sources of malicious traffic … and a filtering process to eliminate the malicious traffic from entering the victim data center." Hence, Greenwald neither describes nor suggest claim 1.

Claims 9, 18, and 21 are allowable over Greenwald for analogous reasons as in claim 1. For example, claim 9 calls receiving … statistical data from a plurality of monitors… with the monitors sending the statistical data collected from the network over a second, different network, that is a physically separate network from the network that the plurality of monitors collect data from.

Claim 9 also requires analyzing … the statistical data from the plurality of monitors to determine network traffic statistics that can identify sources of malicious network traffic and determining … a filtering process to install on devices in the network that the monitors collect data from to inhibit the malicious traffic from entering the victim data center.

Claims 18 and 21 each include similar features as discussed and are allowable for analogous reasons.

The examiner rejected Claims 1, 3, 5-6, 9, 12-13, 18-19 and 21 under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. US 6,735,702.

The examiner contends that:

> **Messmer teaches a central control center (i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks (see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network (see lines 12-15), the customers network is the victim data center.**

Applicant disagrees. As argued by Applicant of record, Messmer fails to teach the feature of a control center to coordinate thwarting attacks on a victim data center … . According to Messmer, the different products in the article are used to identify attacks. The article says nothing about a control center that coordinates thwarting of attacks. Moreover, the article teaches away from this feature by stating that: "Counterpane staffers advise corporations

on how to combat threats but do not make changes to the corporation's equipment." Accordingly, Messmer fails to teach the feature of the … "the computer system executing a process to analyze the statistical data from the plurality of monitors … a process to identify gateways on the monitoring network that are sources of malicious traffic destined for the data center, and a filtering process to eliminate the malicious traffic from entering the victim center."

The examiner's contention that: "… coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack," does not meet the claim language and fails to address the teaching in Messmer that: "Counterpane staffers advise corporations on how to combat threats but do not make changes to the corporation's equipment." If Counterpane staffers advise corporations but do not make changes to the equipment, Counterpane cannot inherently disclose a control center that has a filtering process to identify malicious traffic and eliminate the malicious traffic … .

The examiner also contends that: "… Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center (see lines 23-28)." Applicant contends that this discussion still does not meet the claim language as recited in claim 1 of "a communication device, coupled to a physically separate network from the network that the data center is coupled."

The mere fact that Messmer teaches that "monitors are on the customers network (12-26)," does not meet "the physically separate network" limitation because Messmer fails to show that the data collected on those networks is transferred to the central control center in California or Virginia without using part of the network that is being monitored.

The examiner acknowledges that Messmer is silent on, filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. The examiner relies on Yavatkar et al. In particular the examiner contends that Yavatkar et al. discloses:

> **analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2), by launching an agent and having the agent iteratively identify which of the links on the node on which agent operates accepts a type of traffic, and traversing the identified link to the node across the link**

> **by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Yavatkar et al.'s filtering process and eliminate the malicious traffic from entering the victim data center within the system of Messmer because it would block the attack targeted on the victim's computer. One would have been motivated to do so because it would further secure the victim's system from malicious attack that is sent over the hardened network.**

Yavatkar et al. fail to disclose or suggest the claimed system whether taken alone or in combination with Messmer. Yavatkar in particular fails to describe either a process to identify gateways on the monitoring network that are sources of malicious traffic destined for the data center or a filtering process to eliminate the malicious traffic from entering the victim data center," as claimed.

The examiner pieces elements from Yavatkar et al. that exist in unrelated mechanisms in Yavatkar to concoct filtering for the claimed system. The teachings at Col. 13, line 54 to col. 14, line 32 add nothing to Messmer than what Messmer teaches alone.

As with Messmer, but unlike Applicant's claim 1, Yavatkar discloses that: "A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may move from node to node, tracing the path of the hostile messages from the victim to the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow." However, the device disclosed by Yavatkar is not described as performing any of the claimed functions of claim 1.

In particular for "filtering" examiner relies: "traversing the identified link to the node across the link by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32." While Yavatkar does mention a prior art method, at Col. 13, namely:

> **However, using current methods to identify the gateway which is, in effect, the source of attack traffic to the network can be difficult and time consuming. A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may move from node to node, tracing the path of the hostile messages from the victim to**

the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow.

Yavatkar teaches away from any combination of a "sniffer" device arguing that it is a conventional method and is slow. However, even the disclosed sniffer does not meet the claim language of "a filtering process to eliminate the malicious traffic from entering the victim data center."

Accordingly, Messmer taken with Yavatkar fail to describe or suggest the claimed invention.

Applicant contends that dependent claims 3 and 5 add distinct features, for reasons of record, and that claim 6 is allowable at least for the reasons discussed in the base claim.

Claims 9, 12-13, 18-19, 21 are patentable for analogous reasons as those given for claims 1, 3 and 5.

The examiner also rejected claims 7-8, 14-16, and 24-25 under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. USPN 6,735,702 B1 and further in view of Hill et al.

These claims add the limitation that the analysis process classifies attacks and determines a response based on the class of attack (Claims 7, 14, 24) or classes of attack denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing (Claims 8, 15, 25). There is nothing in Messmer or Yavatkar that suggests an analysis process that determines a response based on the class of attack, which the examiner acknowledges. The examiner relies on Hill for this teaching. However, Hill does not solve any of the deficiencies in the combination of Messmer and Yavatkar as noted above, and Hill further relates to attack signatures not to the features of the base claims. Therefore, these claims are allowable at least for the reasons discussed in the base claims.

It is believed that all the rejections and/or objections raised by the examiner have been addressed. Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good

reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

Please charge the **$60** Petition for Extension of Time fee to Deposit Account No. 06-1050. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/13/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906